FICHA DE ASIGNATURA

Título: Análisis de Malware

Descripción: El malware es una clase de software cuyo propósito es llevar a cabo diversas acciones en un sistema informático, no deseadas por el usuario legítimo del mismo, generalmente de forma oculta o discreta y que resultan perjudiciales para dicho usuario legítimo o para terceros. El malware hoy en día es usado por organizaciones criminales, gobiernos, agencias de seguridad y otros tantos actores, para muy diversos fines, entre los que destacan la obtención de un rédito económico mediante el robo de datos, operaciones financieras fraudulentas, extorsión, secuestros de datos o espionaje.

Carácter: *Obligatoria*

Créditos ECTS: 4

Contextualización: Comprender qué es el malware, cómo se comporta, cómo se distribuye y cómo evade las medidas de seguridad. Efectuar análisis de muestras de malware (tanto malware para entornos Windows como entornos Android), que permitan al analista obtener información orientada a determinar de qué tipo de amenaza se trata, qué acciones realiza y cuál es su propósito. Para ello se llevarán a cabo análisis de forma estática (sin ejecutarlo) y de forma dinámica (ejecutándolo).

Modalidad: Online

Semana 1

Temario:

Tema 1: Introducción Análisis Malware

1.1 – Qué es el malware

1.2 – Tipos de malware

1.3 – Evolución del malware

1.4 – Estado actual

1.5 – Teoría de las amenazas

1.6 – Casos de estudio

Tema 2: Análisis estático (x86)

2.1 – Introducción

2.2 – Antivirus

2.3 – Packers y crypters (evasión de antivirus)

2.4 – Hashing / fingerprinting

2.5 – Strings

Evaluación Continua:

Ejercicios: Actividad 1 (análisis estático x86)

Semana 2:

Tema 2: Análisis estático (continuación)

2.6 – PE: formato Portable Excecutable

2.7 – Herramientas de análisis estático

Tema 3: Análisis dinámico (x86)

3.1 – Introducción

3.2 – Entorno

3.3 – Herramientas de análisis dinámico

Evaluación Continua:

Ejercicios: Actividad 2 (análisis estático x86)

Semana 3:

Tema 3: Análisis dinámico (continuación)

3.4 – Análisis basado en memoria

3.5 – Análisis basado en debug

3.6 – Análisis basado en sandbox

Tema 4: Análisis en entornos móviles

4.1 – Introducción a las amenazas para dispositivos móviles

4.2 – ThreatIntelligence (Amenazas Móviles)

4.3 – Búsqueda de Malware para Android.

4.4 – Clasificación de Malware para Android.

4.5 – IntelligenceResearch

Evaluación Continua:

Ejercicios: Actividad 3 (análisis dinámico x86)

Ejercicios: Actividad 4 (análisis móviles)

Semana 4:

Tema 4: Análisis en entornos móviles

4.6 – Análisis estático en Android

4.5 – Análisis dinámico en Android

Evaluación Continua:

Competencias*:*

Generales

- CG8 – Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.

Básicas

- CB6 – Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB7 – Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de estos.
- CB8 – Que los estudiantes sepan comunicar sus conclusiones y conocimientos, así como las razones que las sustentan, a públicos especializados y no especializados de una forma clara y sin ambigüedades.
- CB9 – Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de una manera auto-dirigida o autónoma en gran medida.

Transversales

- CT4 – Gestionar la adquisición, estructuración, análisis y visualización de datos e información (en el ámbito informático y de seguridad), y valorar de forma crítica los resultados de esta gestión.
- CT12 – Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (en el ámbito informático y de seguridad) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

Específicas

- CE9 – Capacidad para aplicar métodos matemáticos, estadísticos y de inteligencia artificial para modelar, diseñar y desarrollar aplicaciones, servicios, sistemas inteligentes y sistemas basados en el conocimiento.

Actividades Formativas:

Actividad Formativa	Horas	Presencialidad
Clases Magistrales (Video-Sesiones)	6	100
Clases de Tutoría	6	100
Ejercicios prácticos Individuales	20	0
Estudio autónomo	30	0

Metodologías docentes:

- Clase magistral / método expositivo

- Plataforma virtual de aprendizaje

- Aprendizaje Cooperativo (realización de trabajos)

- Aprendizaje Basado en Problemas (ABP)

- Entornos de simulación (recreación de problemas reales)

Sistema de Evaluación:

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Presentación de trabajos y/o proyectos	15.0	50.0
Examen escrito/oral (prueba objetiva, prueba de respuesta corta y/o prueba de desarrollo).	50.0	50.0

Bibliografía:

1- Practical Malware Analysis

The Hands-On Guide to Dissecting Malicious Software

Michael Sikorsky

Andrew Honig

Google vista previa:

https://books.google.es/books?id=DhuTduZpc4C&printsec=frontcover&hl=es#v=onepage&q&f=false

2.- Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting

Malicious Code

Michael Hale Ligh

Matthew Richard

Steven Adair

Blake Hartstein

3.- Android Malware and Analysis

Ken Dunham, Shane Hartman, Manu Quintans, Jose Andre Morales, Tim

Strazzere

ISBN 9781482252194 - CAT# K23862

Ref: https://www.crcpress.com/Android-Malware-and-Analysis/DunhamHartman-Quintans-Morales-Strazzere/p/book/9781482252194